Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-27 (Cancelled)

Claim 28 (Currently amended): A method of controlling access to electronic information ~~as claimed in claim 1~~ comprising the steps of:

providing at least one user apparatus;

a remote server; and

a communications link between the at least one user apparatus and the remote server;

allocating disk storage space on the remote server unique to the at least one user apparatus;

allowing at least one user access to the storage space via username and password login to the server and via secure encryption of data sent to or from the user apparatus from or to the server; and

allowing at least one further user access to the data storage space and wherein the further users access to the data storage space can be managed by the at least one user with regard to times and dates when the at least one further user can write to and/or read from the data storage space, wherein access to the data storage space by the at least one user is inhibited when the access to the data storage space by the further users is allowed.

Claim 29 (Cancelled)

Claim 30 (New): A method of controlling access to electronic information as claimed in claim 28, wherein the secure encryption comprises:

transactions involving access to the storage space being protected by a requirement for a user to present a digital certificate.

Claim 31 (New): A method of controlling access to electronic information as claimed in claim 30, wherein the digital certificate is required whenever the user attempts to write to or read from the storage space.

Claim 32 (New): A method of controlling access to electronic information as claimed in claim 31, wherein data sent by a user apparatus is encrypted by public key in the case of SSL transactions and additionally by private key via presentation of a digital certificate in the case of accessing the data storage space.

Claim 33 (New): A method of controlling access to electronic information as claimed in claim 32, wherein data received by the server is decrypted via private key in the case of SSL transactions and by public key in the case of digital certificate verification accessing the data storage space.

Claim 34 (New): A method of controlling access to electronic information as claimed in claim 28, wherein each said at least one further user is allowed access to the data storage space upon presentation of a further digital certificate.

Claim 35 (New): A method of controlling access to electronic information as claimed claim 28, wherein the communications link comprises the Internet.

Claim 36 (New): A method of controlling access to electronic information as claimed in claim 30, wherein the secure encryption further comprises transactions between user and server being encrypted using Secure Socket Layer (SSL).

Claim 37 (New): A method of controlling access to electronic information as claimed in claim 28, wherein managing of the at least one further users access to the data storage space by the at least one user involves the at least one user setting at least one date and at least one time period for access by the at least one further users.

Claim 38 (New): An electronic safety deposit system or tender box system comprising:

at least one user apparatus;

a remote server;

a communications link between the at least one user apparatus and the remote server;

disk storage space allocated on the remote server unique to the at least one user apparatus;

means for allowing at least one user access to the storage space via username and password login and via secure encryption of data sent to or from the user apparatus from or to the server;

means for allowing at least one further user access to the data storage space; and

means for managing the further users access to the data storage space by the at least one user with regard to times and dates when the at least one further user can write to and/or read from the data storage space, and further

means for inhibiting access to the data storage space by the at least one user when the access to the data storage space by the further users is allowed.

Claim 39 (New): An electronic safety deposit system or tender box system as claimed in claim 38, wherein the secure encryption comprises transactions involving access to the storage space being further protected by a requirement for a user to present a digital certificate, in use.

Claim 40 (New): A method of providing an account-based Internet/Intranet service which allows an at least one account holder to:

create at least one secure electronic deposit box on a centralised server in which box or boxes store documentation in a secure environment;

manage timeframes for invited participants to access said documentation and/or for the invited participants to upload to the centralised server further documentation, wherein

the method utilizes a method of controlling access to electronic information as claimed in claim 28.

Claim 41 (New): A method as claimed in claim 40, wherein the method further allows the at least one account holder to track activity relating to each said at least one electronic deposit box.

Claim 42 (New): A secure electronic deposit or tender box system comprising an account-based Internet or Intranet server system with a worldwide web (HTTP) interface for uploading and downloading documentation onto a centralised server in a secure environment, using digital certificates to ensure data confidentiality, data integrity, data authentication, non-repudiation and proof of origin and receipt, the system using an electronic safety deposit system as claimed in claim 38.

Claim 43 (New): A programmed computer or server adapted to implement the method of claim 28.

Claim 44 (New): A programmed computer or server adapted to implement the method of claim 40.

Claim 45 (New): A programmed computer or server adapted to implement the method of claim 41.